CLAIMS

1. A process comprising:

storing a first code in a memory of a device, wherein the first code uniquely identifies the device; and

storing encrypted data in the memory, wherein the encrypted data comprises a second code which identifies the device.

2. The process of claim 1 wherein storing the encrypted data on the device comprises:

creating once-encrypted data by encrypting the data using a first encryption key;

encrypting the once-encrypted data using a second encryption key to create the encrypted data; and

storing the encrypted data on the device.

3. The process of claim 2 wherein the first encryption key is a private key and the second encryption key is a private key.

4. The process of claim 1, further comprising:

decrypting the encrypted data using software adapted to operate the device;

comparing the first code to the second code; and

loading the software onto the device if the first code is identical to the second code.

5. The process of claim 4 wherein decrypting the data using the software comprises:

reading the encrypted data from the device;

decrypting the encrypted data using a first decryption key, wherein the result comprises once-decrypted data; and

decrypting the once-decrypted data using a second decryption key.

6. The process of claim 5 wherein the first decryption key is a public key and the second decryption key is a public key.

7. The process of claim 1 wherein the device is a network adapter and the software is a driver adapted to run on the device.

8. An article of manufacture, comprising:

a machine-readable medium having instructions stored thereon to:

store a first code in a memory of a device, wherein the first code uniquely identifies the device; and

store encrypted data in the memory, wherein the encrypted data comprises a second code which identifies the device.

9. The article of manufacture of claim 8 wherein the instructions to store encrypted data in the memory comprise instructions to:

create once-encrypted data by encrypting the data using a first encryption key;

encrypt the once-encrypted data using a second encryption key to create the encrypted data; and

store the encrypted data on the device.

10. The article of manufacture of claim 9 wherein the first encryption key is a private key and the second encryption key is a private key.

11. The article of manufacture of claim 8, wherein the instructions further comprise instructions to:

decrypt the encrypted data using software adapted to run on the device;

compare the first code to the second code; and

load the software onto the device if the first code is identical to the second code.

12. The article of manufacture of claim 11 wherein the instructions to decrypt the encrypted data comprise instructions to:

read the encrypted data from the device;

decrypt the encrypted data using a first decryption key wherein the result comprises once-encrypted data; and

decrypt the once-decrypted data using a second decryption key.

13. The article of manufacture of claim 12 wherein the first decryption key is a public key and the second decryption key is a public key.

14. An apparatus comprising:

a device comprising a memory;

a first code stored in the memory, wherein the code uniquely identifies the device; and

an encrypted data set stored in the memory, wherein the data set comprises a second code which identifies the device.

15. The apparatus of claim 14 wherein the encrypted data set is encrypted a first time with a first encryption key, and the result of the first encryption is encrypted using a second encryption key.

16. The apparatus of claim 15 wherein the first encryption key is a private key and the second encryption key is a private key.

17. The apparatus of claim 14 further comprising software operative with the device to:

decrypt the encrypted data set;

compare the first code to the second code; and

load the software onto the device if the first code and second codes are identical.

18. The apparatus of claim 17 wherein the software being operative with the hardware to decrypt the encrypted data set comprises the software being operative with the device to:

read the encrypted data from the device;

decrypt the encrypted data using a first decryption key, the result being once-decrypted data; and

decrypt the once-decrypted data using a second decryption key.

19. The apparatus of claim 18 wherein the first decryption key is a public key and the second decryption key is a public key.

20. The apparatus of claim 14 wherein the device is a network adapter.

21. The apparatus of claim 14 wherein the memory comprises a non-volatile memory.

22. The apparatus of claim 21 wherein the non-volatile memory is selected from among a group consisting of Electronic Erasable Programmable Read Only Memory (EEPROM), Erasable Programmable Read Only Memory (EPROM), and flash memory.

23. A system comprising:

a computer;

a device comprising a memory, wherein the device is installed in the computer;

a first code stored in the memory, wherein the code uniquely identifies the device; and

an encrypted data set stored in the memory, wherein the data set comprises a second code which identifies the device.

24. The system of claim 23 wherein the encrypted data set is encrypted a first time with a first encryption key, and the result of the first encryption is encrypted using a second encryption key.

25. The system of claim 22 wherein the first encryption key is a private key and the second encryption key is a private key.

26. The system of claim 23 further comprising software operative with the device to:

decrypt the encrypted data set;

compare the first code to the second code; and

load the software into the device if the first code and second codes are identical.

27. The system of claim 26 wherein the software being operative with the hardware to decrypt the encrypted data set comprises the software being operative with the device to:

read the encrypted data from the device;

decrypt the encrypted data using a first decryption key, the result being once-decrypted data; and

decrypt the once-decrypted data using a second decryption key.

28. The system of claim 27 wherein the first decryption key is a public key and the second decryption key is a public key.